ABSTRACT OF THE DISCLOSURE

A method and apparatus are provided for generating a cryptographic key from multiple data sets each related to a respective association of a trusted party and user identity. The cryptographic key is, for example, one of an encryption key, a decryption key, a signature key and a verification key, and is preferably generated by applying Tate or Weil bilinear mappings to the data sets. At least two of the data sets may relate to different user identities and/or different trusted authorities. Where multiple trusted authorities are involved, these authorities may be associated with different elements to which the bilinear mapping can be applied, each trusted authority having an associated public key formed from its associated element and a secret of that trusted authority.